



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,808	05/15/2001	Gerald R. Malan	UOM0234PUS	1533

7590 03/20/2008
David R. Syrowik
Brooks & Kushman P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1351

EXAMINER

FIELDS, COURTNEY D

ART UNIT	PAPER NUMBER
----------	--------------

2137

MAIL DATE	DELIVERY MODE
-----------	---------------

03/20/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte GERALD R. MALAN and FARNAM JAHANIAN

Appeal 2007-3538
Application 09/855,808
Technology Center 2100

Decided: March 20, 2008

Before: LANCE LEONARD BARRY, ALLEN R. MACDONALD, and
CAROLYN D. THOMAS, *Administrative Patent Judges.*

MACDONALD, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. §§ 6(b) and 134(a) from a Final Rejection of claims 1-19, 21-23, and 26-33.

Claim 1 is exemplary:

1. A system for detecting, tracking and blocking one or more denial of service attacks over a computer network, the system comprising:

a collector adapted to receive a plurality of data packet flow statistics from a routing system of the computer network and to process the plurality of data packet flow statistics to detect one or more data packet flow anomalies and to generate a signal representing the one or more data packet flow anomalies; and

a controller coupled to the collector to receive the signal;

wherein the controller is constructed and arranged to respond to the signal by tracking attributes related to the one or more data packet flow anomalies to at least one source,¹ and wherein the controller is constructed and arranged to block the one or more data packet flow anomalies.

The reference relied upon by the Examiner in rejecting the claims on appeal is:

Belissent US 6,789,203 B1 Sept. 7, 2004

Claims 1-19, 21-23, and 26-33 stand rejected under 35 U.S.C. § 102(e) as anticipated by Belissent.

We affirm.

FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

Belissent

1. Belissent discloses identifying an IP address of a denial of service (DoS) attack based on an excessive number of connection requests. (Col. 5, ll. 45-60 and Col. 6, ll. 2-17.)

¹ In our analysis, we refer to “wherein the controller is constructed and arranged to respond to the signal by tracking attributes related to the one or more data packet flow anomalies to at least one source” as the “tracking step.”

2. Belissent discloses that a processor unit 212 determines whether a number of connection requests is excessive by comparing the number to a threshold value, which represents an excessive number of requests. (Col. 5, ll. 49-59 and Col. 5, l. 66 – Col. 6, l. 17.)
3. Belissent discloses that when the number of requests is excessive, processor 212 identifies the excessive requester as an attacker and processor 212 directs throttler unit 216 to refuse new connections from the attacker. (*Id.*)

PRINCIPLES OF LAW

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

For a prior art reference to anticipate in terms of 35 U.S.C. § 102, every element of the claimed invention must be identically shown in a single reference. However, this is not an "ipsissimis verbis" test and the reference need not use the same terms to be within the scope of what is claimed. *In re Bond*, 910 F.2d 831, 832 (Fed. Cir. 1990).

ANALYSIS

Claims 1, 19, and 27

Claims in this group are subject to the same rejection. Appellants group these claims together under the same heading and set forth the same

arguments of Examiner error for these claims. (App. Br. 6-8.) Therefore, we select claim 1 as the representative claim to decide the appeal of all claims in this group.

The Examiner finds that Belissent anticipates claim 1. (Ans. 3-4 and 9-10.) Appellants allege that Belissent does not anticipate claim 1 because Belissent does not disclose the tracking step. (App. Br. 7.) In particular, Appellants argue that:

Contrary to the Examiner's assertion, “tracking” or “*tracing*” of the present invention is not equivalent to either “identifying” or “detecting” a denial service attack. Only the present invention describes and claims tracking one or more denial of service attacks *over a computer network*, as emphasized at numerous locations in the specification and claims. Such “tracking” or “*tracing*” is only done after detecting data packet flow anomalies or a DoS attack.

(App. Br. 7-8 (emphases added).)

Thus the issue is whether Appellants have shown that the Examiner erred in finding that Belissent discloses the tracking step.

Appellants’ arguments are based on features that are not required by claim 1. Claim 1 does not recite “tracing.” Claim 1 recites, in pertinent part, “denial of service attacks *over a computer network*” (emphasis added) in its preamble. We find that “over a computer network” refers to the denial of service attacks and not tracking. Thus, because Appellants arguments do not address the limitations in claim 1, we find that Appellants have not shown that the Examiner erred in finding that Belissent discloses the tracking step.

Moreover, we find that Belissent discloses the tracking step for reasons provided *infra*. Appellants’ Specification provides no explicit

definition of “tracking.” However, Appellants’ Specification provides examples of *tracing* that involve identifying the source of an attack. (Spec. 17:25 – 18:13.) Accordingly, we broadly yet reasonably construe the claimed tracking step to require identifying the source of an attack.

We find that Belissent discloses identifying an IP address of a DoS attacker. (FF 1.) The IP address identifies the source of the attack. Accordingly, we find that Belissent discloses identifying the source of an attack and thus meets a requirement of the claimed tracking step.

The tracking step also requires identifying the source of an attack *in response to* a signal that represents a data packet flow anomaly. We find that Belissent discloses that processor unit 212 identifies the attacker in response to determining that a number of connection requests is excessive. (FF 2 and 3.) We find that a determination of an excessive number of requests meets the claimed signal representing a data packet flow anomaly. Accordingly, we find that Belissent’s identifying the excessive requester as an attacker *in response to* a determination of excessive requests discloses identifying the source of an attack *in response to* a signal that represents a packet flow anomaly. Thus, we do not find that Appellants have shown that the Examiner erred in finding that Belissent discloses the tracking step. Accordingly, we sustain the Examiner’s rejection of claim 1 and claims 19 and 27 under 35 U.S.C. § 102(b) over Belissent.

Other Claims

With regard to dependent claims 2-18, 21-23, 26, and 28-33, other than stating that those claims stand rejected, Appellants make no allegation that the Examiner erred in finding the dependent claims anticipated by

Belissent. (App. Br. 2, 6, and 8.) Accordingly, because Appellants make no arguments of Examiner error, we find that Appellants have not shown that the Examiner erred in finding the dependent claims anticipated by Belissent.

CONCLUSION OF LAW

We conclude that:

(1) Appellants have not shown that the Examiner erred in finding that that claims 1-19, 21-23, and 26-33 are unpatentable under 35 U.S.C. § 102(e) for being anticipated by Belissent and

(2) Claims 1-19, 21-23, and 26-33 are unpatentable.

DECISION

The Examiner's rejection of claims 1-19, 21-23, and 26-33 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

pgc

David R. Syrowik
Brooks & Kushman P.C.
1000 Town Center, 22nd Floor
Southfield MI 48075-1351